Unit 11: Cyber Security and Incident Management – mark grid

General marking guidance

- All learners must receive the same treatment. Examiners must mark the first learner in exactly the same way as they mark the last.
- Marking grids should be applied positively. Learners must be rewarded for what they have shown they can do rather than be penalised for omissions.
- Examiners should mark according to the marking grid, not according to their perception of where the grade boundaries may lie.
- All marks on the marking grid should be used appropriately.
- All the marks on the marking grid are designed to be awarded. Examiners should always award full marks if deserved. Examiners should also be prepared to award zero marks if the learner's response is not rewardable according to the marking grid.
- Where judgment is required, a marking grid will provide the principles by which marks will be awarded.
- When examiners are in doubt regarding the application of the marking grid to a learner's response, a senior examiner should be consulted.

Specific marking guidance

The marking grids have been designed to assess learner work holistically.
Rows within the grids identify the assessment focus/outcome being targeted. When using a marking grid, the 'best fit' approach should be used.

- Examiners should first make a holistic judgement on which band most closely matches the learner response and place it within that band. Learners will be placed in the band that best describes their answer.
- The mark awarded within the band will be decided based on the quality of the answer in response to the assessment focus/outcome and will be modified according to how securely all bullet points are displayed at that band.
- Marks will be awarded towards the top or bottom of that band depending on how they have evidenced each of the descriptor bullet points.

PART A, Activity 1 – Risk assessment of the networked system

Assessment focus	Band 0	Band 1	Band 2	Band 3	Max mark
Activity 1: Risk assessment of the networked system	**0**	**1–3**	**4–6**	**7–8**	**8**
	No awardable content.	Demonstrates superficial understanding of security threats. Risk assessment shows limited interpretation of the scenario, using generic reasoning to identify some obvious and/or common threats. Risk assessment provides generally unreasonable and/or unrealistic judgements of: • risk severity • risk probability • size of potential loss.	Demonstrates sound understanding of security threats. Risk assessment shows reasoned interpretation of the scenario, using some logical chains of reasoning to identify an adequate range of threats. Risk assessment provides mostly reasonable and realistic judgements of: • risk severity • risk probability • size of potential loss.	Demonstrates in-depth understanding of security threats. Risk assessment shows perceptive interpretation of the scenario, using logical chains of reasoning to identify a comprehensive range of threats. Risk assessment provides consistently reasonable and realistic judgements of: • risk severity • risk probability • size of potential loss.	

PART A, Activity 2 – Cyber security plan for the networked system

Assessment focus	**Band 0**	**Band 1**	**Band 2**	**Band 3**	**Band 4**	**Max mark**
Activity 2: Cyber security plan for the networked system	**0**	**1–5**	**6–10**	**11–15**	**16–20**	**20**
	No awardable content.	Report identifies limited measures that provide little or no protection against few threats. Report includes reasons for actions that demonstrate a limited understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a limited understanding of the protection measure in relation to the threat(s) covering: • constraints • legal responsibilities • usability • cost-benefit. Test plan is limited and includes few relevant tests and/or actions.	Report identifies some measures that provide basic protection against the most common threats. Report includes reasons for actions that demonstrate a basic understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a basic understanding of the protection measure in relation to the threat(s) covering: • constraints • legal responsibilities • usability • cost-benefit. Test plan is basic and includes some relevant tests and/or actions.	Report identifies adequate measures that are mostly effective in protecting the system against an adequate range of threats. Report includes reasons for actions that demonstrate a sound and logical understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a sound understanding of the protection measure in relation to the threat(s) covering: • constraints • legal responsibilities • usability • cost-benefit. Test plan is adequate and includes mostly relevant tests and actions.	Report identifies robust measures that effectively protect the system against a comprehensive range of appropriate threats. Report includes reasons for actions that demonstrate comprehensive and in-depth understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a comprehensive understanding of: • constraints • legal responsibilities • usability • cost-benefit. Test plan is comprehensive and includes relevant tests and actions throughout.	

Part A, Activity 3 – Management report justifying the solution

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 3: Management report justifying the solution	0	1–3	4–6	7–9	10–12	12
	No awardable content.	Alternative security protection measures, if identified, are likely to be inappropriate.	Appropriate alternative security protection measures are identified for some aspects of the security plan.	Appropriate alternative security protection measures are identified for a range of aspects of the security plan.	Appropriate alternative security protection measures are identified for a range of aspects of the security plan.	
		Demonstrates limited understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures.	Demonstrates a basic understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures.	Demonstrates a sound understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures.	Demonstrates a comprehensive understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures.	
		Limited justification that refers to the risk assessment and security plan to address a few of the security requirements.	Basic justification that refers to the risk assessment and security plan to address some of the security requirements.	Sound and mostly logical justification that integrates aspects of the risk assessment and security plan to address most of the security requirements.	Comprehensive and logical justification that integrates aspects of the risk assessment and security plan to fully address the security requirements.	

PART A, Activity 1–3 – Use of technical language during the task

Assessment focus	Band 0	Band 1	Band 2	Band 3	Max mark
Activity 1–3: Use of technical language	0	1	2	3	3
	No awardable content.	Limited appropriate use of technical language.	Mostly appropriate technical language with some inconsistencies.	Appropriate and consistent technical language used throughout.	

PART B, Activity 4 – Forensic incident analysis

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 4: Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident and come to a conclusion about the probable cause(s) of the security incident.	**0**	**1–3**	**4–7**	**8–11**	**12–14**	**14**
	No awardable content.	Response demonstrates a limited understanding of the forensic procedures and how a few pieces of evidence were obtained. Superficial analysis of evidence, with incomplete links between the pieces of evidence and/or back to the scenario. Conclusion, if present, lacks support or plausibility, with little or no consideration of alternative possibilities.	Response demonstrates a basic understanding of forensic procedures and how some of the evidence was obtained. Reasoned analysis of the evidence, showing generally logical chains of reasoning that link some of the evidence together and back to the scenario. Conclusion is plausible and partially supported, with an unbalanced consideration of alternative possibilities.	Response demonstrates a sound understanding of forensic procedures and how most of the evidence was obtained. Sound analysis of the evidence, showing logical chains of reasoning that link most of the evidence together and back to the scenario. Conclusion is sound and mostly supported, with a generally balanced consideration of alternative possibilities.	Response demonstrates a comprehensive understanding of forensic procedures and how the evidence was obtained throughout. Perceptive analysis of the evidence, showing logical chains of reasoning that comprehensively link the evidence together and back to the scenario. Conclusion is convincing and fully supported, with a balanced consideration of alternative possibilities.	

PART B, Activity 5 – Management report on security improvements

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 5: Review the incident and suggest ways to prevent a similar incident in the future.	**0**	**1–5**	**6–10**	**11–15**	**16–20**	**20**
	No awardable content.	Review shows limited analysis, identifying generic weaknesses with incomplete or imbalanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are mostly unrealistic in the context of the scenario and would not reduce the likelihood of a similar incident. Justification is limited and lacks support, showing a superficial understanding of the incident.	Review shows basic analysis, identifying a few appropriate weaknesses with imbalanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are occasionally realistic in the context of the scenario and would reduce the likelihood of a similar incident. Justification is mostly valid and partially supported with some logical chains of reasoning, showing a basic understanding of the incident.	Review shows sound analysis, adequately identifying appropriate weaknesses with generally balanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are mostly realistic in the context of the scenario and would reduce the likelihood of a similar incident. Justification is valid and mostly supported with logical chains of reasoning, showing a sound understanding of the incident.	Review shows perceptive analysis, comprehensively identifying appropriate weaknesses with balanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are realistic in the context of the scenario and would greatly reduce the likelihood of a similar incident. Justification is valid and fully supported with logical chains of reasoning, showing an in-depth understanding of the incident.	

PART B, Activity 4–5 – Use of technical language during the task

Assessment focus	Band 0	Band 1	Band 2	Band 3	Max mark
Activity 4–5: Use of technical language	**0**	**1**	**2**	**3**	**3**
	No awardable content.	Limited appropriate use of technical language.	Mostly appropriate technical language with some inconsistencies.	Appropriate and consistent technical language used throughout.	